

United States Section Directive

Volume: I I
Chapter: 901
Date: October 01, 2005

Subject: USIBWC Manual of Security Policies and Procedures

To: All USIBWC Managers and Supervisors
Presidents, AFGE Locals 3060 & 3309

Control: Chief Security Officer

901.1 Requirement/Authority.

The Security Manual implements the laws, regulations, Executive Orders, and directives that govern management and administration of the personnel, information, and physical security programs of the USIBWC and outlines the policies, procedures, and general standards to guide security efforts to protect the Commission's employees, property, facilities, and information. The head of each Federal agency is responsible for establishing and sustaining programs for the protection of resources assigned to the agency; this includes personnel and property. Of particular importance is the administration of a program providing a reasonable degree of security for agency employees and visitors, physical structures, and equipment. This manual supercedes all other manuals; specifically the one dated July 29, 2003.

901.2 Purpose.

The purpose for this directive is to establish the basic outline for ensuring a reasonable degree of security for the agency's human and physical resources to include emergency management planning and workplace violence prevention. Planning for security is a management responsibility and shall be an integral part of any function or project undertaken in the USIBWC. Managers and supervisors are responsible for ensuring the security of USIBWC employees, property, facilities, and information in their respective organizations in accordance with applicable laws, regulations, Executive Orders, and directives. The Chief Security Officer provides security advice, assistance, guidance, consultation, and services to assist Project/Facility Managers in performing their security responsibilities.

901.3 Responsibilities.

The primary responsibility for ensuring the security of USIBWC resources rests with the United States Commissioner. Delegated assignments designed to ensure this responsibility is met are as follows:

Principal Engineer - Operations: Responsible for the implementation of security program requirements for the USIBWC.

Legal Advisor: Responsible for providing legal counsel to agency personnel engaged in developing and implementing security program policy and provisions.

Chief Security Officer: Responsible for providing policy oversight and subject matter guidance to USIBWC management officials regarding security, to include emergency management planning and workplace violence prevention.

Security Officers: Responsible for carrying out officially assigned security enforcement duties in a professional manner as members of the agency's security force and for adhering to the provisions of this directive, the Physical Security Officer Policy Manual, and supplemental orders and procedures. The organizational title of "security officer" is to be used to those personnel who officially are classified as a Security Guard, GG-0085. Except for official personnel and pay purposes, "security officer" is the title to be used when referring to such personnel.

901.4 Related Issuances.

Various directives and other guidance pertaining to the security of USIBWC human, fiscal, and physical resources have been issued. Guidance that has not been consolidated into this directive will continue to be followed.

901.5 Supplemental Manuals.

A. Security Manual.

1. A security manual is to be established for each of the following organizational units and will be a supplement to this directive. Project/Facility Managers will utilize the HQ's Manual as a template. Further information as described in paragraph 901.6 below.

- a. Headquarters Security Manual: M901-HQ-1-1 (Section 1- Chapter 1);
- b. Lower Rio Grande Flood Control Project Security Manual (to include specific provisions for Anzalduas Dam and Retamal Dam); M901-LRG;
- c. Falcon Dam Project Security Manual: M901-FDP;

- d. Amistad Dam Project Security Manual: M901-ADP;
- e. Presidio Project Security Manual: M901-PP;
- f. Upper Rio Grande Flood Control Projects Security Manual (to include specific provisions for American Dam Facility, Zac Dominguez Field Office, and Las Cruces Field Office): M900-URG;
- g. Nogales Sanitation Project: M901-NSP;
- h. Yuma Project: M901-YP: and
- i. San Diego Project: M901-SDP.

2. The project/facility manager of each of the above-referenced projects will assume primary responsibility for the development and annual review of the project's security manual. The Chief Security Officer will assume primary responsibility for the development and annual review of the headquarters security manual and assist the project/facility managers.

3. The security manual will include the following essential elements:

a. Emergency Management Plan. The physical security manual will include an emergency management plan, the purpose for which is twofold: to provide a useful framework for coping responsively with a variety of emergency situations that could occur; and to assign personnel responsibilities to manage such emergencies.

b. While the format of the security manual will include the above-referenced essential element, its content will be at the discretion of the management official responsible for developing the manual. Maximum flexibility in the content is in recognition of the unique security requirements facing each organizational unit.

4. The Security Manual will be available to all USIBWC employees. It is "For Official Use Only" and will not be released to the public.

5. The security manual should be completed not later than 180 calendar days following the issuance of this directive. The manual will be provided, through the chain of command, to the Chief Security Officer. The Project/Facility Manager should conduct an annual review of the manual and make revisions as deemed necessary.

6. A Project/Facility Manager with a dam facility will continue to develop and update an emergency action plan handbook, which will be separate and distinct from the security manual, as directed by the chief of the Operations and Maintenance Division. These procedures will address a detrimental release of water.

B. Security Officer Manual.

The Security Officer Manual is applicable to those field offices staffed with USIBWC security officers. It also is applicable to some extent to the USIBWC headquarters building, which is provided limited services by Upper Rio Grande Project security officers who secure the building and turn designated alarms on and off each duty day.

901.6 **Supersession.**

The various individual emergency action plans and agency protection action plans, which have been developed will be superseded as replacement manuals are developed and issued.

901.7 **Effective Date.**

This directive will be effective immediately following its issuance.

FOR THE COMMISSIONER

//original signed//
Kenneth Rakestraw
Principal Engineer - Operations



Manual of Security Policies and Procedures

Foreword

The events of September 11th, 2001 have forever altered the way in which the United States views and responds to its security. The Commissioner of the United States Section, International Boundary and Water Commission (USIBWC), is committed to providing a safe and secure working environment for employees, contractors, and the visiting public to the maximum extent possible. The Manual of Security Policies and Procedures ("Security Manual") is issued under the authority of the Commissioner, USIBWC. It implements the laws, regulations, Executive Orders, and directives that govern the administration and management of the personnel, information, and physical security programs of the USIBWC and outlines the policies, procedures, and standards to guide security efforts to protect USIBWC employees, property, and facilities. The provisions of the Security Manual apply to all USIBWC operating units, offices, facilities, employees, contractors, and others who have access to our facilities, information, personnel, or IT systems.

Section I outlines the Security Administration and focuses on security authorities, responsibilities, applications, and security education and awareness. Section II prescribes policies, procedures, and standards of physical security measures designed to protect employees, property, facilities, and information. Section III is the Information Technology Handbook, and Section IV (under construction) will provide guidance on the protection of sensitive, but unclassified, information and other security matters. The security field is a continuously evolving arena. The Security Manual should be regarded as a "living" document, i.e.: it may change at any time to adapt to new situations, circumstances, procedures, and technologies.

Planning for security is a management responsibility and must be an integral part of any function or project undertaken in our agency. Project/Facility/Site Managers, Heads of operating units and Departmental offices are responsible for ensuring the security of the personnel, property, facilities, and information in their respective organizations in accordance with applicable laws, regulations, Executive Orders, and directives. The Chief Security Officer provides security advice, assistance, guidance, consultation, and services to assist the Managers, heads of operating units and Departmental offices in performing their security responsibilities.

//original signed//

T.J. Smith
Chief Security Officer
28 February 2006

Manual of Security Policies and Procedures



M901-HQ

Table of Contents

Supplement to:

Volume: II

Chapter: 901

Section I – Security Administration

CHAPTER 1 SECURITY AUTHORITIES AND APPLICATION

- 101 Purpose
- 102 Authority
- 103 Delegation of Authority
- 104 Statuses and Applicability of the Security Manual
- 105 Security Manual Issuance
- 106 Supplementary Requirements and Guidance
- 107 Interpretation and Requests for Exceptions

CHAPTER 2 SECURITY RESPONSIBILITIES

- 201 Security Planning
- 202 Roles and Responsibilities
- 203 Administrative and Judicial Action
- 204 After Hours Security Checks and Self Inspections

CHAPTER 3 SECURITY EDUCATION AND AWARENESS

- 301 Security Education and Awareness
- 302 Security Briefings

CHAPTER 4 SECURITY INSPECTIONS AND ASSISTANCE

- 401 Purpose
- 402 Inspection Procedures and Frequency of Compliance Reviews
- 403 Self Inspection

CHAPTER 5 INCIDENT REPORTING

- 501 Incident Reporting System
- 502 Reporting Procedures

CHAPTER 6 EMERGENCY PLANNING AND EVACUATION

- 601 Emergency Planning
- 602 Phased Security Procedures

CHAPTER 7 FOREIGN TRAVEL

- 701 Travel Security
- 702 Conduct and Reporting Requirements

Section II – Physical Security

CHAPTER 1 PHYSICAL SECURITY POLICIES

- 101 Purpose
- 102 Application
- 103 Policies

CHAPTER 2 PHYSICAL SECURITY PLANNING

- 201 Security Planning
- 202 Facility Protection
- 203 Planning Facility Protection
- 204 Design Factors
- 205 Surveys and Inspections

CHAPTER 3 EXTERIOR PROTECTION

- 301 Perimeter Security Measures
- 302 Fencing
- 303 Gates
- 304 Protective Lighting
- 305 Perimeter Intrusion Detection
- 306 Doors
- 307 Windows
- 308 Manholes, Grates, and Storm Drains
- 309 Roof Openings
- 310 Shafts, Vents, and Ducts
- 311 Fire Escapes and Building Walls
- 312 Signage

CHAPTER 4 INTERIOR PROTECTION

- 401 Interior Security Controls
- 402 Area Designations
- 403 Challenge Authority
- 404 Property Control
- 405 Intrusion Detection Systems
- 406 Security Vaults
- 407 Strongrooms

CHAPTER 5 IDENTIFICATION AND ADMITTANCE TO FACILITIES

- 501 Identification
- 502 Forms of Identification
- 503 Procedures for Issuance and Removal
- 504 Admittance to USIBWC Facilities
- 505 Exceptions

CHAPTER 6 LOCKS AND KEYS

- 601 Security Requirements
- 602 Types of Devices
- 603 Changing a Combination
- 604 Keys

CHAPTER 7 GUARD SERVICES

- 701 Determining the Need
- 702 Typical Guard Duties
- 703 Personnel Requirements
- 704 Supervision
- 705 Contracting for Guard Services
- 706 Guard Force Standard Operating Procedures
- 707 Guard Force Management

CHAPTER 8 COMPUTER SYSTEMS AND FACILITIES

- 801 Protection of Automated Information Systems
- 802 Facility Design
- 803 Walls and Windows
- 804 Doors and Locking Hardware
- 805 Access Control
- 806 Fire Protection
- 807 Data Storage Areas

Section III – Information Technology

SEE ATTACHED DIRECTIVE DATED 10/25/2005

Section IV – Classified/Sensitive Information Security

UNDER CONSTRUCTION

Appendices

- A - Glossary of Acronyms and Terms
- B - Workplace Violence
- C - Weapons
- D - Security Officers Manual
- E - Department of Justice Standards for Facility Security
- F - Sample Security Memorandum
- G - Facility Security Checklist
- H - Security Checklist for Personal Computer Users
- I - Sample Emergency Management SOP
- J - Sample Access Control SOP
- K - Sample General Evacuation SOP
- L - Sample Key and Lock Control SOP
- M - Sample Bomb Threat SOP
- N - Sample SOP for Security of Property and Equipment
- O - Sample Facility Closure SOP
- P - Sample Natural Disaster SOP
- Q - Sample Civil Disturbance SOP
- R - Sample Restricted Areas SOP